REMARKS

This amendment is responsive to the Office Action[1] having a mailing date of June 27, 2005. Claims 1-6 and 8-22 were presented for examination in this RCE application and have been rejected. All independent claims, namely claims 1, 5, 9, 13, 14 and 22, are currently amended. Support for these amendments can be found in the application as originally filed. For example, see Fig. 1 and the specification, at least page 5, line 18 through page 6, line 15, discussed on page 13 herein; no new matter is added. No claims are canceled. No claims are added. Thus, claims 1-6 and 8-22 are pending.

The Office Action states that these claims have been re-examined and a further search has been performed. Claims 1-6 and 8-22 are rejected under 35 U.S.C. § 102(b) as being anticipated by Sudia et al. (U.S. Patent No. 5,825,880; hereinafter Sudia). This rejection is the same as the last rejection, based on Sudia, implying that no better art was found. The rejection is respectfully traversed because all claim elements of the independent claims are not disclosed or suggested by Sudia, for the following reasons.

Consider currently amended claim 1:

> In a node operative within a network of a plurality of nodes, a method for performing cryptographic-related functions, comprising: executing an application program at the *node* which is *not highly secured*; receiving an input requiring cryptographic-related processing; generating a message via the application program based on the input, the message representing one of a predefined set of messages for *processing by a cryptographic processing component located within the node*; transmitting the message to the cryptographic processing component; and performing the cryptographic-related processing by the cryptographic processing component. (Emphasis added.)

[1] The Office Action may contain a number of statements characterizing the cited references and/or the claims which Applicants may not expressly identify herein. Regardless of whether or not any such statement is identified herein, Applicants do not automatically subscribe to, or acquiesce in , any such statement.

Claim 1 calls for, interalia, (1) executing an application program at a node that *isn't highly secured* and (2) processing a message generated from the application program by a *cryptographic processing component located within the node*. But, Sudia does not disclose or suggest executing an application program at a node which is not highly secured while processing a message by a cryptographic processing component located within that node. The Office Action, page 3, refers to Sudia, col. 7, lines 53-65 to show "within the node" processing. Although such processing, *arguendo*, may be shown, to the contrary, *this section calls for a highly secure environment*. It says: "Although less preferred, the signing device 39 and message server 47 could be implemented as separate tasks on a single computer *in a highly secure environment*." (col. 7, lines 62-65, Emphasis added.)

Therefore, Sudia does not disclose or suggest claim 1 because to the extent it teaches processing a message generated from the application program by a cryptographic processing component within the node, under those conditions it calls for a highly secure environment while Applicants' claim recites that its node is not highly secured. In other words, for a message processed by a cryptographic component located within a node which also executes an application program in Applicants' claim, that node is not highly secure, but in Sudia it is highly secure. Indeed, Sudia does not disclose or suggest at least the claimed combination including Applicants executing and generating steps: "executing an application program at the node which is not highly secured; receiving an input requiring cryptographic-related processing; generating a message via the application program based on the input, the message representing one of a predefined set of messages

for processing by a cryptographic processing component located within the node" as recited in claim 1.

With further reference to claim 1, the Office Action, page 3 states:

> "[(col. 3, lines 28-29 and col. 7, lines 33-34) A 'node which need not be highly secured' can broadly interpret as a node that involves some kind of security which does not mean the node or the environment is unprotected. The limitation 'not to be highly secured' does not read the same as a node is not secured or unprotected. Hence, Sudia's network includes a node that is not highly secured because the node contains some kind of protection when it is requested to perform cryptographic related processing such as the signing device involving public/private keys.]"

The undersigned representative telephoned the Examiner on August 16, 2005 with respect to obtaining a clarification of this Office Action language. As best understood, this language is interpreted to mean that a node which need not be highly secured can still be secured to some extent. Applicants agree with that logical interpretation. That interpretation, however, which Applicants believe was irrelevant even prior to the current amendment, is now certainly irrelevant because currently amended claim 1 recites "is not highly secured." Furthermore, the last sentence in the above-quoted language, as well as the cites of col. 3, lines 28-29 and col. 7, lines 33-34 are discussing Sudia operation when server 47 is *separate* from signing device 39 as shown, e.g., in Fig. 2, and as described, e.g., in column 7, line 23, and not when signing device 39 and message server 47 are implemented on a single computer as described in column 7, lines 62-65. Therefore, it is respectfully submitted that that last sentence is also irrelevant to Applicants' currently amended claim 1 which calls for processing by a cryptographic processing component located within the same node that is executing the application program.

Applicants' amendment language, "...the node is not highly secured" is supported by the application as originally filed. For example, in Applicants' specification, page 6, lines 1-3, it discusses the nodes 110, 120, and 130 of Fig. 1, such nodes along with server 140 and network 150 comprising Applicants' system. As stated therein, those nodes can be any type of computer device. For example, as disclosed therein, those nodes can be "a personal computer, a laptop, a personal digital assistant (PDA) or a similar device with a connection to network 150." Clearly, these examples of nodes from which Applicants' claimed subject matter can be implemented are not used in a highly secure environment - e.g., people using a laptop or a PDA do not first find their way to a "vault" and then place themselves with their laptop or PDA inside the vault for security purposes before operating their laptop or PDA. Far to the contrary, laptops and PDA's are used in virtually all public spaces such as, for example, airports, airplanes, trains and train stations, buses and bus depots, taxis, hotels lobbies, corporate business environments, etc. Therefore, Applicants' specification as originally filed clearly supports the notion that the "nodes" of its system are used without their being highly secured, as recited in amended claim 1.

Sudia itself reinforces the fact that personal computers and the like are operated in unsecured areas. "Fig. 3 illustrates a working station for authorizing agents. The human operators who act as authorizing agents may work in relatively *unsecured* areas at desk-top [personal] computers or terminals 51 typically found in a business office." (Sudia, column 8, lines 20-23, Emphasis added.)

It is respectfully submitted that Sudia does not anticipate claim 1 because it does not disclose or suggest at least the claimed combination including Applicants' executing

and generating steps: "executing an application program at the node which is not highly secured; receiving an input requiring cryptographic-related processing; generating a message via the application program based on the input, the message representing one of a predefined set of messages for processing by a cryptographic processing component located within the node" as recited in claim 1 for reasons stated above. (Emphasis added.) MPEP § 2131 states that to anticipate a claim, the reference must teach every element of the claim. Since at least these claim elements are not taught by Sudia, it is respectfully requested that the rejection of claim 1 under 35 USC § 102(b) be withdrawn and the claim allowed.

The other independent claims 5, 9, 13, 14 and 22 have been similarly amended, where each independent claim contains a similar limitation relating to its equivalent node (i.e., equivalent to the node which performs the method of Applicants' claim 1) that it is not highly secured. Therefore, the other independent claims are urged to be likewise allowable for reasons similar to those given above.

It is respectfully submitted that claims 2-4 dependent from claim 1, claims 6 and 8 dependent from claim 5, claims 10-12 dependent from claim 9, and claims 15-21 dependent from claim 14 are also allowable, at least for reasons based on their dependencies from allowable base claims. Furthermore, these dependent claims are independently allowable because they recite additional features not disclosed or suggested by Sudia as detailed in a previous response dated June 29, 2004, where those reasons need not be repeated here.

Therefore, in view of the foregoing, it is respectfully submitted that all independent and dependent claims are allowable over cited reference Sudia.

CONCLUSION

In view of the foregoing amendments and remarks, the Applicants respectfully request withdrawal of the outstanding rejections and the timely allowance of this application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-2347 and please credit any excess fees to such deposit account.

Respectfully submitted,

By: _____
Joel Wall
Reg. No. 25,648

Date: September 19, 2005
Verizon Corporate Services Group Inc.
600 Hidden Ridge Drive
Mail Code HQE03H14
Irving, Texas 75038
(972) 718-4800
CUSTOMER NO. 32127